2019 年度情報セキュリティ大学院大学 ProSec メインコース対象演習の内容

■CSIRT 運営管理者向けメインコース（CS-M2019）の対象となる演習

演習名	演習内容	必修・選択	開講日程・時間帯
CSIRT 実践（CSIRT 構築の手引き、NW セキュリティ技術、Web アプリ検査、デジタルフォレンジック）	[CSIRT 構築の手引き]（5/30、5/31） セキュリティインシデント対応の基本的なプロセス、および対応時に用いられる技術について、解説と演習を通して習得するほか、組織内でのインシデント対応組織（CSIRT）の立上げと運用、および CSIRT 連携の進め方についてケーススタディを通して学びます。また、現実に起きている攻撃手法のデモや Web サーバのログ解析演習を通して、サイバー攻撃によるインシデントの実例について学びます。 [NW セキュリティ技術]（6/27、6/28） 検査ツールを利用したサーバに対するポートスキャン検査演習と脆弱性検査演習を行うとともに、発見された脆弱性を是正するための対策演習を行い、結果を報告書にまとめる演習を実施します。 [Web アプリケーション検査]（7/4、7/5） 脆弱性を持つ Web サーバが設置された環境を利用し、主要な検査項目の演習を集中して行うとともに、対策の提案を含む検査結果報告書をまとめる演習を実施します。 [デジタルフォレンジック]（7/17、7/18、7/19） デジタルフォレンジックの基礎知識・技術の解説、Windows 端末の解析で共通的に実施される基本的な作業に関する解説と実習、企業におけるインシデントを想定した本格的な解析演習を集中して行うとともに、結果を報告書にまとめる演習を実施します。	必修	5/30（木）、5/31（金）、6/27（木）、6/28（金）、7/4(木)、7/5(金) 7/17（水）、7/18（木）、7/19（金）　各日とも 9:40～17:00（1 コマ 90 分×4 コマ×9 日）（計 54 時間）
セキュアシステム技術演習―NW 攻撃とその防御および検知―	攻撃者がどのようなツールや手法を用いてネットワーク不正侵入行為を行うか、またどのような防御方法や検知方法が有効かについて、講義と実習を通して理解を深めます。また、その上で、セキュアなシステムの構築方法についても学びます。主な演習項目は、以下の通りです。 ネットワーク経由での各種情報収集／脆弱性検査／ Windows バッファオーバーフロー／Web アプリケーションに対する攻撃／マルウェアとその検出等	選択	10/21(月)、10/22(火)、10/23(水)、10/28(月)、10/29(火)、10/30(水) 各日とも 9:00～17:50(1 コマ 90 分×5 コマ×6 日）（計 45 時間）

■IoT セキュリティメインコース（IO-M2019）の対象となる演習

演習名	演習内容	必修・選択	開講日程・時間帯
IoT セキュリティ実践演習	[組込システムの基礎]（6/4） IoT デバイスを開発するために基礎となるハードウェアとソフトウェアの基礎知識を習得します。主な講義・演習項目は、以下の通りです。 組込システムを構成するハードウェア要素／組込システムの実世界インタフェース／mbed による組込デバイス開発 [IoT アーキテクチャ]（6/5、6/6） IoT のビジョンとアーキテクチャを従来型の IT と比較しながら考察し、その違いによって生じる IoT のセキュリティリスクを理解し、システムに存在するリスクや脅威を予測する方法を学修します。主な 講義・演習項目は、以下の通りです。 IoT の概念と特徴、IoT のレイヤアーキテクチャ、IoT のセキュリティ事象／IoT ネットワーク、LPWA／IoT システムの運用と規格・認証／IoT を取り巻く法制度／車載エレクトロニクス、制御システムネットワーク／IoT デバイスの信頼の基点、TrustZone, Trusted Secure IP／セキュア IoT デバイス演習 [IoT システムの脅威分析と脆弱性検査演習]（6/11、6/12） IoT システムのセキュリティを開発・展開前に十分に検討することができるように、リスクを想定し、対策する計画を立てる脅威分析技術やそのツールを学修します。主な講義・演習項目は、以下の通りです。 機能安全／セキュリティバイデザインとセキュリティ要求分析手法／脅威分析手法と脆弱性検査／スマートホームのセキュリティ要求分析演習／スマートホームの脅威分析演習／スマートホームの脆弱性検査演習	必修	6/4（火）、 6/5（水）、6/6（木）、 6/11（火）、6/12(水) 各日とも 9:40～17:00(1 コマ 90 分×4 コマ×5 日）（計 30 時間）
セキュアシステム技術演	攻撃者がどのようなツールや手法を用いてネットワーク不正侵入行為	必修	10/21(月)、10/22(火)、

習―NW 攻撃とその防御および検知―	を行うか、またどのような防御方法や検知方法が有効かについて、講義と実習を通して理解を深めます。また、その上で、セキュアなシステムの構築方法についても学びます。主な演習項目は、以下の通りです。ネットワーク経由での各種情報収集／脆弱性検査／ Windows バッファオーバーフロー／Web アプリケーションに対する攻撃／マルウェアとその検出等		10/23(水)、10/28(月)、10/29(火)、10/30(水) 各日とも 9:00～17:50(1 コマ 90 分×5 コマ×6 日)（計 45 時間）

■企業経営向けビッグデータ分析とリスク経営メインコース（RM-M2019）の対象となる演習

演習名	演習内容	必修・選択	開講日程・時間帯
インシデント対応と CSIRT 基礎演習	本演習では、セキュリティインシデント対応の基本的なプロセス、および対応時に用いられる技術について、解説と演習を通して習得します。また、組織内でのインシデント対応組織（CSIRT）の立上げと運用、および CSIRT 連携の進め方についてケーススタディを通して学びます。	必修	8/20(火)、8/21(水)、8/22(木)、8/23(金)、8/27(火)、8/28(水)、8/29(木) 8/23(金) は 13:00 ～ 17:50。他は 18:20～21:30 （計 22.5 時間）